

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
29 September 2005 (29.09.2005)

PCT

(10) International Publication Number
WO 2005/091546 A3

(51) International Patent Classification⁷: **H04L 9/00**, [US/US]; 2115 Emerson Avenue South, Minneapolis, MN 55405 (US).

(21) International Application Number: PCT/US2005/008521

(22) International Filing Date: 15 March 2005 (15.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: 10/801,070 15 March 2004 (15.03.2004) US

(71) Applicant (for all designated States except US): **CARDIAC PACEMAKERS, INC.** [US/US]; 4100 Hamline Avenue North, St. Paul, MN 55112-5798 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HEALY, Scott J.** [US/US]; 6295 Juneau Lane North, Maple Grove, MN 55311 (US). **QUILES, Sylvia** [US/US]; 6512 Wilryan Avenue, Edina, MN 55439 (US). **VON ARX, Jeffrey A.**

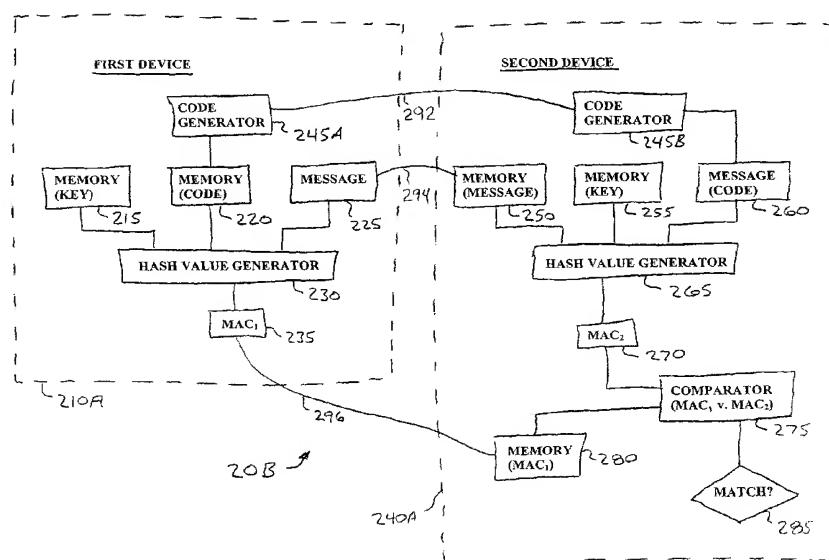
(74) Agents: **STEFFEY, Charles E.** et al.; Schwegman, Lundberg, Woessner & Kluth, P.A., P.O. Box 2938, Minneapolis, MN 55402 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: CRYPTOGRAPHIC AUTHENTICATION FOR IMPLANTABLE MEDICAL DEVICE TELEMETRY



WO 2005/091546 A3

(57) Abstract: Integrity of a wirelessly telemetered message communicated between an implantable medical device and an external programmer is authenticated by encoding the message. The message is encrypted based on a random number or time stamp and a secret key. The message is authenticated by encryption and decryption or by executing a hash function.



Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(88) Date of publication of the international search report:

17 November 2005

INTERNATIONAL SEARCH REPORT

International Application No
US2005/008521A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/00 A61N1/372

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L A61N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/074036 A1 (PRUTCHI DAVID ET AL) 17 April 2003 (2003-04-17) paragraph '0047! -----	1-18
Y	PATENT ABSTRACTS OF JAPAN vol. 2003, no. 05, 12 May 2003 (2003-05-12) & JP 2003 022008 A (SONY CORP), 24 January 2003 (2003-01-24) abstract -----	1-18
Y	US 2003/114897 A1 (VON ARX JEFFREY A ET AL) 19 June 2003 (2003-06-19) paragraphs '0035!, '0074!; figure 1 -----	19-59
Y	US 5 737 419 A (GANESAN ET AL) 7 April 1998 (1998-04-07) column 5, paragraph 2 ----- -/-	19-24, 31-46

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

° Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

21 September 2005

Date of mailing of the international search report

11.10.2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Authorized officer

Edward, V

INTERNATIONAL SEARCH REPORT

onal Application No
JS2005/008521

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/065919 A1 (ALBERT ROY DAVID ET AL) 3 April 2003 (2003-04-03) paragraph '0065! - paragraph '0072! -----	25-30, 47-59
A	US 2003/159048 A1 (MATSUMOTO TSUTOMU ET AL) 21 August 2003 (2003-08-21) paragraph '0050! -----	1-59
A	US 6 028 527 A (SOENEN ET AL) 22 February 2000 (2000-02-22) column 18, paragraph 1 column 21, line 1 - line 5 -----	1-59
A	US 2002/120838 A1 (ABDULKADER BARBIR) 29 August 2002 (2002-08-29) paragraphs '0006!, '0018! -----	1-59
A	US 5 898 397 A (MURRAY ET AL) 27 April 1999 (1999-04-27) column 3, paragraph 8 -----	1-59

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2005/008521

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

The additional search fees were accompanied by the applicant's protest.

No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-18

A device with communications of high data integrity achieved by hash value comparison.

2. claims: 19-24, 31-46

A system with communications of high secrecy and immunity to replay attacks achieved by the use of encryption in combination with a code.

3. claims: 25-30, 47-59

A system with communications of high data integrity and immunity to replay attacks achieved by use of hash value comparison in combination with a code.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

US2005/008521

Patent document cited in search report	Publication date	Patent family member(s)			Publication date
US 2003074036	A1	17-04-2003			NONE
JP 2003022008	A	24-01-2003			NONE
US 2003114897	A1	19-06-2003	AU 2002364179 A1		09-07-2003
		EP 1458444 A1			22-09-2004
		WO 03053515 A1			03-07-2003
US 5737419	A	07-04-1998	US 5535276 A		09-07-1996
US 2003065919	A1	03-04-2003	EP 1386444 A1		04-02-2004
		JP 2004532468 T			21-10-2004
		WO 02087143 A1			31-10-2002
US 2003159048	A1	21-08-2003	CN 1439982 A		03-09-2003
		JP 2003244139 A			29-08-2003
		SG 108889 A1			28-02-2005
US 6028527	A	22-02-2000	NONE		
US 2002120838	A1	29-08-2002	CA 2330166 A1		29-06-2002
US 5898397	A	27-04-1999	US 5699065 A		16-12-1997